JURNAL INFORMATIKA
Vol. 12, No 2, July 2018, pp. 45-52
ISSN: 1978-0524

Combination and comparison of AES and RC4 cryptography in least significant bit (LSB) method in digital image to improve message security

Rahmat Sulaiman,

STMIK Atma Luhur, Jl. Jend. Sudirman, Kel. Selindung, Pangkalpinang 33172, Indonesia
rahmatsulaiman@atmaluhur.ac.id

ABSTRACT

Message security is something that must be kept secretly. However, to maintain the security and the secret of a message it takes two different methods. To maintain the security of messages, the science that has been widely used is to use cryptography. As for maintaining the secret of the message, the science used is steganography. For that, we need a security message that can maintain the security and the secret of the message simultaneously. Various algorithms have been widely applied in data security, but it is unknown which algorithm has a superior speed when applied in the LSB. The test is done by calculating the length of the encryption time process and the decryption time process of each algorithm with the same number of messages and key lengths. Measurement time is done as much as 10 times, then taken average value to get consistent time because system instability. Therefore, we will compare the speed of encryption and decryption process by applying AES and RC4 algorithm to LSB in Visual Studio 2008. In the process of encryption and decryption, the AES algorithm is superior in terms of speed compared to RC4 algorithm. The MSE and PSNR values generated from the encrypted images based on the AES and RC4 algorithm doesn't show significant value. Overall the AES algorithm is better than RC4 algorithm when applied in LSB.

Keywords:
Cryptography
Steganography
LSB
AES
RC4

I. Introduction

Communicating with each other is a basic human need, whether oral or written. Communication becomes the main way to do everything, both in conveying information and to simply exchanging opinions. The more rapid the development of technology today, the problem of information security given to be the main concern because the confidentiality of information between the sender and the recipient must be maintained. In this case, cryptography and steganography help humans in securing the exchange of information made. Symmetric cryptography has a faster processing speed compared to the use of asymmetric key cryptography because the mathematical calculations used in the encryption and decryption process are the same [1].

Nowadays is highly dependent on Computer Technology, especially personal and a group (organization). Almost in every activity, the organization requires computerization in its operation. In the case of the use of computerization, it is made a safeguard for all its assets, especially information and important data in order to maintain the confidentiality of the data information. A data security system becomes a demand that must be available for data security systems to be better in securing data from various threats that may arise. This is the background of the development of data security system that serves to protect data transmitted or transmitted through a communication network.

II. Related Work

Data security is important in an enterprise. Security and integrity of data is something that must be considered. Efforts to keep information from falling into the hands of unauthorized persons demanding the need to apply a good mechanism insecurity. There are many common cryptographic methods can be applied, in the classification generally consists of two, Symmetric and Asymmetric

DOI: 10.26555/jifo.v12i2.a8667
W : http://journal.uad.ac.id/index.php/JIFO
E : jifo@uad.ac.id

method. In this project, carried out an analysis in the perspective of data security and computational complexity using two types of cryptography methods, for its implementation, created a system where data is transmitted (plaintext) first encrypted by the sender generate encrypted data (ciphertext) and will be sent to the receiver to do the decryption process to produce a data intact as before [2].

Security and confidentiality of data is currently a very important issue and continues to grow. Some cases involving data security is now a job that requires handling and security costs so much. To maintain the security and confidentiality of messages, data, or information that cannot be read or understood by any person, except for recipients who are entitled, then the application of a safety system designed by the method of data encryption using the RC4 algorithm.RC4 (Rivest Cipher 4) is a Synchrony stream cipher, which has a symmetric key cipher and encrypt the plaintext digits are digits per byte by byte or by combining with a binary operation XOR with a random number [3].

With rapidly telecommunications and computer also allows users to store the data digitally. In this case, the problem of security and confidentiality of data is a very important thing, it must be protected for confidential data purpose. A technique within the science of cryptography is one way that can secure data from disturbance of others. Cryptography is the art of securing the message into a message that is not recognized. Also known as Rijndael Advanced Encryption Standard (AES) is a cryptographic encryption algorithm used. However, by using the method can still give rise to a suspicion, for securing data safely and not to arouse suspicion. The use of steganography the least significant bit (LSB) to be one the better choice. Least significant bit is a method to insert a piece of confidential information in an object other media such as image or jpg. This method does not cause major changes to the images that are used by naked eye [4]. While cryptography is the science that studies how to keep data or messages stay safe when shipped, from the sender to the receiver without the interference of others. The purpose of this study is to provide maximum security to the digital image, using steganography method Least Significant Bit (LSB) and the cryptographic algorithm RC4 stream cipher. The expected outcome of this research is to secure the application of digital image [5].

III. RC4 and AES

RC4 has a S-Box, S0, S1, ..., S255 which brutally permutated from the numbers 0 to 255. In the encryption algorithm, this method will generate pseudorandom bytes of the key which will be subjected to XOR operation against the plaintext to generate ciphertext (Figure 1).

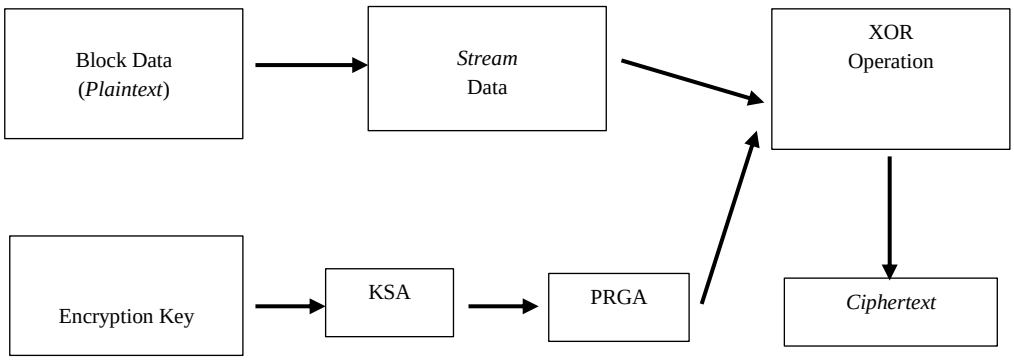

Fig. 1. Encryption Process Diagram of RC4

To show how the RC4 algorithm works, Figure 2 explained using four-bit keys, to make it look simple.

```
Array S                 Array K
0 1 2 3                  2 5 7 3
i = 0
j = (0 + S[0] + K [0 mod 4]) mod 4 = (0 + 0 + 2) mod 4 = 2
Swap (S[0],S[2])
2 1 0 3
i = 1
j = (2 + S[1] + K [1 mod 4]) mod 4 = (2 + 1 + 5) mod 4 =0
Swap (S[1],S[0])
1 2 0 3
i = 2
j = (0 + S[2] + K [2 mod 4]) mod 4 = (0 + 0 + 7) mod 4 = 3
Swap (S[2],S[3])
1 2 3 0
i = 3
j = (3 + S[3] + K [3 mod 4]) mod 4 = (3 + 0 + 3) mod 4 = 2
Swap (S[3],S[2])
1 2 0 3
Array S
1 2 0 3
i = 0,       j = 0
i = (0 + 1) mod 4 = 1
j = (0 + S[1]) mod 4 = (0+ 2) mod 4 = 2
swap (S[1],S[2])
1 0 2 3
K1 = S[(S[1]+S[2]) mod 4] = S[2 mod 4] = 2
K1 = 00000010
i = (1 + 1) mod 4 = 2
j = (2 + S[2]) mod 4 = (2+ 2) mod 4 = 0
swap (S[2],S[0])
2 0 1 3
K2 = S[(S[2]+S[0]) mod 4] = S[3 mod 4] = 3
K2 = 00000011
i = (2 + 1) mod 4 = 3
j = (0 + S[3]) mod 4 = (0+ 3) mod 4 = 3
swap (S[3],S[3])
1 0 2 3
K3 = S[(S[3]+S[3]) mod 4] = S[6 mod 4] = 2
K3 = 00000010
i = (3 + 1) mod 4 = 0
j = (3 + S[0]) mod 4 = (3+ 1) mod 4 = 0
swap (S[0],S[0])
1 0 2 3
K1 = S[(S[0]+S[0]) mod 4] = S[2 mod 4] = 2
K1 = 00000010
HALLO :
01001000 01000001 01001100 01001111
Key        :
00000010 00000011 00000010 00000010
Ciphertext          :
01001010 01000010 01001110 01001101
(L)                 (B)       (N)       (M)
```

Fig. 2. RC4 algorithm example

With 128-bit data, Nb = 4 (Nb = plaintext block length is dived by 32 and Nk = key length divided by 32) indicating the data length of each line is 4 bytes. With 128-bit input or data block

blocks, the keys used in the AES algorithm should not have the same magnitude as the input blocks. Cipher key on the AES algorithm can use a 128-bit, 192-bit, or 256-bit key (Table 1). The key length difference will affect the number of rounds that will be implemented on this AES algorithm.

Table 1. AES Key

	(Key)	**(Block)**	**(Round)**
AES – 128	4	4	10
AES – 192	6	4	12
AES – 256	8	4	14

Decryption steps for Rijndael algorithm:

1. In the decryption process known is only the key, the existing key is expanded first, the process is the same as the encryption in order to obtain RoundKey.
2. Ciphertext is XORed with the last RoundKey obtained from the Key Schedule process. This process is called Inverse of AddRoundKey
3. Ciphertext results from the AddRoundKey process shifted the second line to the right of 1 step, the third line 2 steps to the right, and so on until the fourth line = 3 steps to the right. This process is called Inverse of ShiftRow
4. Ciphertext generated from the Inverse of ShiftRow process is then transformed into a specified Inverse S-Box box. This process is called inverse of SubBytes.
5. The transformed ciphertext is then XORkan with the specified matrix.
6. The result of Inverse of MixColumn is XORed with RoundKey next round. And so on until the last round.

IV. Experimental

Implementation Encryption and Decryption for 100 characters with 6 digits key by using algorithm Rc4 and AES (Figure 3).

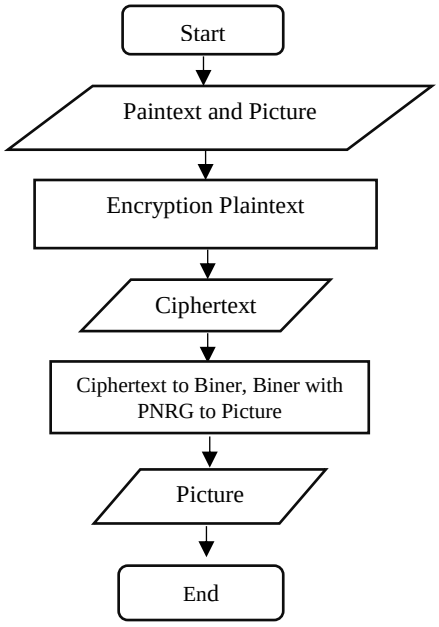

Fig. 3. Encryption Process

Based on the flowchart on Figure 3, this section is trying to encryption 100 character with RC4 Algorithm and AES Algorithm (Figure 4).

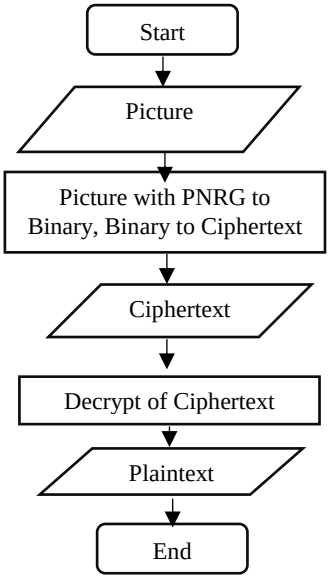

Fig. 4. Decryption Process

This section is trying to Decryption 100 character with RC4 Algorithm and AES Algorithm. Table 2 and Figure 5 illustrate the length of time the encryption process for RC4 and AES algorithms which is applied to the LSB method. The x-axis represents the number of encrypted characters and the y-axis representing the length of the encryption process in milliseconds. The test was done 10 times for each number of characters, the values are representing the average value of time process. This is done to get consistent time, given the unstable processor performance during the time measurement process. Based on the graph, the encryption process with the AES algorithm takes less time than the RC4 algorithm.

Table 2. Encryption Time

Characters	Encryption Time (Millisecond)	
	RC4	AES
100	6	1.4
200	6.3	1.6
300	7.2	1.9
400	7.8	2
500	8.4	2
600	8.8	2.1
700	9.4	2.3
800	10.3	2.5
900	10.6	2.5
1000	11.1	2.7

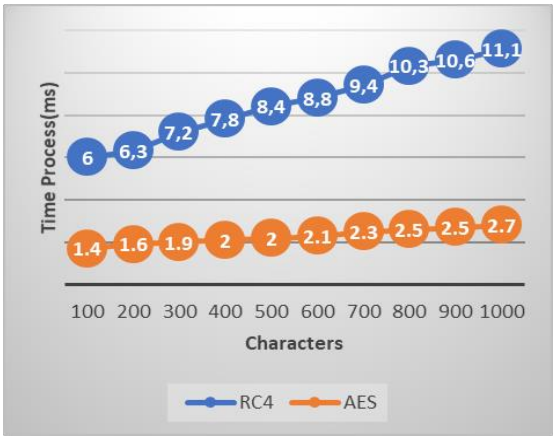

Fig. 5. Chart of Encryption Time

Table 3 and Figure 6 illustrate the length of decryption time for RC4 and AES algorithms applied to the LSB method. The x-axis represents the number of encrypted characters and the y-axis representing the length of the encryption process in milliseconds. The test is done 10 times for each number of characters, the value entered into the graph is the average value. This is done to get consistent time, given the unstable processor performance during the time measurement process. Based on the graph, the encryption process with the AES algorithm takes less time than the RC4 algorithm.

Table 3. Decryption Time

Characters	Decryption Time (Millisecond)	
	RC4	AES
100	646.3	63.6
200	1377.8	133.1
300	2219.6	195.2
400	3134.8	258.8
500	4151.1	320.9
600	5345.8	401.7
700	6684.8	463.2
800	8130	530.7
900	9733.9	595.6
1000	11582	662

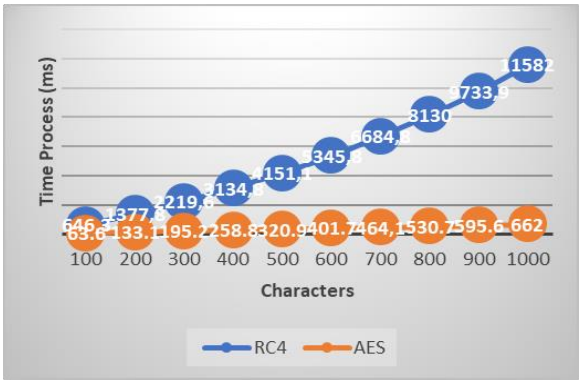

Fig. 6. Chart of Decryption Time

After encryption a picture with several characters based on RC4 or AES algorithm, the pictures contains secret message have value of MSE and PSNR (Table 4 and Table 5). In this section Value of MSE and PSNR will be show based on how many characters inside the pictures. To implement data hiding to a pictures or images. The text that has bees encrypted must be converted into bytes and the PRNG will spread it into bytes at the pictures or images. Then the pictures has MSE and PSNR, MSE and PSNR willshow us, how good the pictures or images after contains secret message.

Table 4. MSE of Pictures (RC4 and AES)

Characters	RC4 MSE	AES MSE
100	38.1781	37.813
200	38.2248	38.0855
300	38.3687	38.132
400	38.4302	38.4423
500	38.5769	38.5523
600	38.7548	38.6434
700	38.9389	38.4482
800	39.1587	38.9822
900	39.2893	39.1988
1000	39.4443	39.4875

Table 5. PSNR of Pictures (RC4 and AES)

Characters	RC4 PSNR	AES PSNR
100	32.2944	32.3038
200	32.2733	32.3002
300	32.2688	32.2957
400	32.2635	32.2876
500	32.2591	32.2831
600	32.2504	32.2724
700	32.2491	32.2605
800	32.2449	32.2541
900	32.2353	32.231
1000	32.2252	32.2143

Table 4 and Table 5 illustrate the Mean Square Error (MSE) value and Peak Signal to Noise Rtio value of the resulting image based on the RC4 algorithm and the AES algorithm.

V. Conclusion

Based on the results of the analysis conducted, testing and test results from research that has been done, then the conclusions obtained, namely as follows:

1. AES algorithm has superior speed in encryption process and decryption process compared with RC4 algorithm when applied in Steganography.
2. The speed of the encryption and decryption process depends on the number of characters encrypted and decrypted.
3. The number of characters encrypted in the image affects the value of MSE and PSNR produced, although not significant.
4. As the results of calculations in Table show that insertion of a text message with different sizes will result in different MSE and PSNR values. The larger the message file size the MSE value will be greater and the smaller the PSNR value, and vice versa the smaller the message file size the smaller the MSE value and the greater the PSNR value

References

[1] Cheddad, A., Joan, C., Curran, K. & Paul, M.K. 2010, Digital image steganography: Survey and analysis of current methods Signal Processing 90

[2] Basri. 2016, *Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi*, Program Studi Teknik Informatika Universitas Al Asyariah Mandar, Jurnal Ilmiah Ilmu Komputer, Vol. 2, No. 2, September 2016

[3] Elka LH., Khairil dan Fery HU. 2014, *Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4 Dengan Menggunakan Bahasa Pemrograman PHP*, Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu, Jurnal Media Infotama Vol. 10 No. 1, Februari 2014

[4] Adetya, K.P. *Pengamanan Data Dengan Metode Advanced Cryption Standard dan Metode Least Significant Bit*, Mahasiswa Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semaran

[5] Utsav S. & Shiva S. 2016, *Image Steganography Using AES Encryption and Least Significant Nible*¸ International Conference on Communication and Signal Processing,, India

[6] Nurhayati & Syukuri, S.H. 2014,*Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm*, Informatics Engineering Department, Science and Technology Faculty Syarif Hidayatullah State Islamic University (UIN) Jakarta,.

[7] Gede, W.B, & Made, I.W.2015, *Implementasi Algoritma Kriptografi AES 256 dan Metode Steganografi LSB pada Gambar Bitmap*, Jurnal Ilmiah Ilmu Komputer, Universitas Udayana, Vol. 8, No. 2, September 2015

[8] N.P, Indah, F.A. & Awang, H.K. 2015, Jurnal Implementasi Kriptografi Pengamanan Data Pada File Teks, Isi File Dokumen dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. Jurnal Informatika Mulawarman Vol. 10 No.1